All Saints Nursery School

E- Safety Policy

Date written: November 2022
Date of last update: October 2023
Date agreed and ratified by Trustees, November 2023
Date of next full review: November 2024

E-safety Policy (including all electronic devices with internet capacity)

All Saints Nursery School

Online Safety

It is important that children and young people receive consistent messages about the safe use of technology and are able to recognise and manage the risks posed in both the real and the virtual world.

Terms such as 'e-safety', 'online', 'communication technologies' and 'digital technologies' refer to fixed and mobile technologies that adults and children may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks. The issues are:

Content – being exposed to illegal, inappropriate or harmful material

Contact – being subjected to harmful online interaction with other users

Conduct – personal online behaviour that increases the likelihood of, or causes, harm

I.C.T Equipment

- The setting manager ensures that all computers have up-to-date virus protection installed.

- Tablets are only used for the purposes of observation, assessment and planning and to take photographs for individual children's learning journeys.

- Tablets remain on the premises and are stored securely at all times when not in use.

- Staff follow the additional guidance provided with the system

Internet access

Staff

- The DSL has overall responsibility for online safeguarding within the setting but will liaise as necessary with other members of staff

- All Saints Nursery School uses a wide range of technology. This includes computers, laptops, tablets and other digital devices, the internet, our online learning journal, email and invoicing systems.

All setting owned devices and systems will be used with appropriate safety and security measures in place.

- All Saints Nursery School will do all we reasonably can to limit exposure to online risks through our IT systems and will ensure that appropriate filtering and monitoring systems are in place.
-
    - Systems are password protected and staff have separate logins
        - If learners or staff discover unsuitable sites or material, they are required to report the concern immediately to a member of staff, report the URL of the site to technical staff/services.
    - All users will be informed that use of our systems can be monitored, and that monitoring will be in line with data protection, human rights, and privacy legislation.
    - Filtering breaches or concerns identified through our monitoring approaches will be record and reported to the DSL (or deputy), Manager and technical staff as appropriate.

- o Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the [Internet Watch Foundation](#) and the police.
- All Saints Nursery School will ensure that online safety training for staff is integrated, aligned and considered as part of our overarching safeguarding approach.

- The DSL will respond to online safety concerns in line with the child protection and other associated policies.
  - o Internal sanctions and/or support will be implemented as appropriate.
  - o Where necessary concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.

Children

- Children never have unsupervised access to the internet.

- The setting manager ensures that risk assessments in relation to e-safety are completed.

- Only reputable sites with a focus on early learning are used (e.g., CBeebies).

- Video sharing sites such as YouTube are viewed before sharing with children due to the risk of inappropriate content. These are only used for educational research activities

- Children are taught the following stay safe principles in an age-appropriate way:

  - ⁃ only go online with a grown up

  - ⁃ be kind online **and** keep information about me safely

  - ⁃ only press buttons on the internet to things I understand

  - ⁃ tell a grown up if something makes me unhappy on the internet

- Staff support children's resilience in relation to issues they may face online, and address issues such as staying safe, appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.

- All computers for use by children are sited in an area clearly visible to staff.

- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.

The setting manager ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

Personal mobile phones – staff and visitors (includes internet enabled devices)

- Personal mobile phones and internet enabled devices are not used by staff during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place e,g, staff room. The setting manager completes a risk assessment for where they can be used safely.

- Personal mobile phones are switched off and stored in lockers or a locked office drawer.

- In an emergency, personal mobile phones may be used in the privacy of the office with permission.

- Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.

- Staff do not take their mobile phones on outings.

- Members of staff do not use personal equipment to take photographs of children.

- Parents and visitors do not use their mobile phones on the premises. There is an exception if a visitor's company/organisation operates a policy that requires contact with their office periodically throughout the day. Visitors are advised of a private space where they can use their mobile.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the setting.

- Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development, or for displays, and are only taken on equipment belonging to the setting.

- Camera and video use is monitored by the setting manager.

- Where parents request permission to photograph or record their own children at special events, general permission is first gained from all parents for their children to be included. Parents are told they do not have a right to photograph or upload photos of anyone else's children.

- Photographs/recordings of children are only made if relevant permissions are in place.

- If photographs are used for publicity, parental consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed in a sweatshirt with the name of their setting on it.

Cyber Bullying

If staff become aware that a child is the victim of cyber-bullying at home or elsewhere, they discuss this with the parents and refer them to help, such as: NSPCC Tel: 0808 800 5000 www.nspcc.org.uk or ChildLine Tel: 0800 1111 www.childline.org.uk

Use of social media

Staff are expected to:

- understand how to manage their security settings to ensure that their information is only available to people they choose to share information with

- ensure the organisation is not negatively affected by their actions and do not name the setting

- are aware that comments or photographs online may be accessible to anyone and should use their judgement before posting

- are aware that images, such as those on Snapshot may still be accessed by others and a permanent record of them made, for example, by taking a screen shot of the image with a mobile phone

- observe confidentiality and refrain from discussing any issues relating to work

- not share information they would not want children, parents or colleagues to view

- set privacy settings to personal social networking and restrict those who are able to access

- not accept service users/children/parents as friends, as it is a breach of professional conduct

- report any concerns or breaches to the designated person in their setting

- not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the practitioner and family are friendly prior to the child coming to the setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed

Use/distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images and that it is an offence to groom children online. In the event of a concern that a colleague is behaving inappropriately, staff advise the designated person who follow procedure Allegations against staff, volunteers or agency staff.